

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A computer implemented method of detecting
- 2 scanning attacks, comprises:
- 3 adding host-pair connection records to a ~~connection table~~first data
- 4 structure stored on a computer readable medium when a host accesses another
- 5 host during a first update period;
- 6 ~~at the end of a first update period, accessing the connection table to~~
- 7 ~~determine new host pairs;~~ determining the number of new host pairs added to the
- 8 ~~connection table~~first data structure over the first update period; ~~and~~
- 9 aggregating host-pair connection records from the first data structure into
- 10 a second data structure which corresponds to a second update period that is
- 11 greater than the first update period;
- 12 determining the number of new host pairs added to the second data
- 13 structure over the second update period; and
- 14 indicating a host as a scanner when at least one of the following
- 15 conditions is true:
- 16 (1) if the host has made appears in more than a first threshold number
- 17 “C1” of host pairs within the first update period, and an a first historical number of
- 18 host pairs is smaller than the first threshold number by a first factor value; “C2”
- 19 and
- 20 , then

21 (2) the host appears in more than a second threshold number of host pairs
22 within the second update period, and a second historical number of host pairs is
23 smaller than the second threshold number by a second factor value.

1 2. (Currently amended) The method of claim 1 wherein “C1” and “C2”
2 first threshold number and the first factor value are adjustable thresholds.

1 3. (Currently amended) The method of claim 2 wherein the ~~connection~~
2

<u>first data structure</u>

 is a current time-slice connection table and ~~host-pair~~
3

<u>pair connection</u>

 records are added to the current time slice connection table.

1 4. (Currently amended) The method of claim 3, further comprising:
2 ~~aggregating records from the current time slice table into a second update~~
3 ~~period table, the second update period table having a period that is greater in~~
4 ~~duration than the first update period;~~
5 checking for ping scans at the end of the second update period; and
6 indicating hosts which produced more than “C3”~~the second threshold~~
7 number of new host pairs over the second update period.

1 5. (Cancelled)

1 6. (Currently amended) The method of claim 1 further comprising:
2 maintaining Address Resolution Protocol (ARP) packet statistics in the
3 ~~connection table~~

<u>first data structure</u>

 and for sparse subnets tracking the number of
4 generated ARP requests that do not receive responses to detect scans on sparse
5 sub-networks.

1 7. (Original) The method of claim 1 wherein the scanning attack is a ping
2 scanning attack.

8. (Currently amended) A computer implemented method of detecting port scanning attacks, the method comprises:

retrieving from a ~~connection table~~first data structure stored on a computer readable medium logged values of protocols and ports ~~used in host-pair~~host-pair connections-connection records added in the connection-tablefirst data structure during a first update period;

determining the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;
aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period;

determining the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

reporting a host associated with a port scan when at least one of the following conditions is true:

(1) the number of ports associated with the host within the first update period is greater than a first threshold number, and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value; and
determining if the number of ports used in an historical profile is smaller by a factor "C1" than a current number of ports being scanned by a host; and if the current number is greater than a lower bound threshold "C2" recording an anomaly; and

reporting a port scan

(2) the number of ports associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.

1 9. (Original) The method of claim 8 further comprising:
2 assigning a severity level to the port scan and reporting the severity level
3 of the port scan.

1 10. (Original) The method of claim 8 wherein the reported severity varies
2 as a function of the deviation from historical norm.

1 11. (Currently amended) The method of claim 8 further comprising:
2 determining from accessing data in the ~~connection table~~first data structure,
3 statistics about TCP reset (RST) packets and ICMP port-unreachable packets, to
4 detect a spike in the number of RST packets and ICMP port-unreachable packets
5 ~~relative to the historical profile to increase~~determine the severity of a port scan
6 event.

1 12. (Cancelled)

1 13. (Cancelled)

1 14. (Currently amended) A computer program product residing on a
2 computer readable medium for detecting scanning attacks, comprises instructions
3 for causing a computer to:

4 add host-pair connection records to a ~~connection table~~first data structure
5 when a host accesses another host during a first update period;

6 ~~at the end of a first update period, accessing the connection table to~~
7 ~~determine new host pairs;~~

8 determine the number of new host pairs added to the ~~connection table~~first
9 data structure over the first update period; ~~and~~

10 aggregate host-pair connection records from the first data structure into a
11 second data structure which corresponds to a second update period that is greater
12 than the first update period;
13 determine the number of new host pairs added to the second data structure
14 over the second update period; and
15 indicate a host as a scanner when at least one of the following conditions
16 is true:
17 _____ (1) the host appears in more than a first threshold number of host pairs
18 within the first update period, and a first historical number of host pairs is smaller
19 than the first threshold number by a first factor value; and
20 _____ (2) the host appears in more than a second threshold number of host pairs
21 within the second update period, and a second historical number of host pairs is
22 smaller than the second threshold number by a second factor value, if a host has
23 made more than a first threshold number “C1” host pairs, and an historical
24 number of host pairs is smaller than the threshold number by a first factor value
25 “C2”, then
26 indicate to a console that the new host is a scanner.

1 15. (Currently amended) The computer program product of claim 14
2 wherein the first threshold number and the first factor value “C1” and “C2” are
3 adjustable thresholds.

1 16. (Currently amended) The computer program product of claim 14
2 wherein the ~~connection table~~ first data structure is a current time-slice connection
3 table and ~~host pair~~ host-pair connection records are added to the current time slice
4 connection table.

1 17. (Currently amended) The computer program product of claim 16,
2 further comprising instructions to:

3 ~~aggregate records from the current time slice table into a second update~~
4 ~~period table;~~
5 check for ping scans at the end of a the second update period; and
6 indicate hosts which produced more than “C3”~~the second threshold~~
7 number of new host pairs over the second update period.

1 18. (Cancelled)

1 19. (Currently amended) The computer program product of claim 14
2 further comprising instructions to:
3 maintain Address Resolution Protocol (ARP) packet statistics in the
4 ~~connection table~~first data structure; and
5 track the number of generated ARP requests that do not receive responses
6 to detect scans on sparse sub-networks.

1 20. (Currently amended) A computer program product residing on a
2 computer readable medium for detecting port scanning attacks, the computer
3 program product comprises instructions for causing a processor to:
4 retrieve from a ~~connection table~~first data structure logged values of
5 protocols and ports ~~used for in host-pair~~host-pair connection records ~~connections~~
6 in the ~~connection table~~first data structure during a first update period;
7 determine the number of ports associated with a host over the first update
8 period based on the host-pair connection records in the first data structure;
9 aggregate host-pair connection records from the first data structure into a
10 second data structure which corresponds to a second update period that is greater
11 than the first update period;
12 determine the number of ports associated with a host over the second
13 update period based on the host-pair connection records in the second data
14 structure; and

15 report a host associated with a port scan when at least one of the following
16 conditions is true:
17 (1) the number of ports associated with the host within the first update
18 period is greater than a first threshold number, and a first historical number of
19 ports associated with the host is smaller than the first threshold number by a first
20 factor value; and
21 (2) the number of ports associated with the host within the second update
22 period is greater than a second threshold number, and a second historical number
23 of ports associated with the host is smaller than the second threshold number by a
24 second factor value;
25 determine if the number of ports used in a historical profile is
26 smaller by a factor "C1" than a current number of ports being scanned by a host
27 and the current number is greater than a lower bound threshold "C2", to record
28 the anomaly; and
report a port scan to a console.

1 21. (Original) The computer program product of claim 20 further
2 comprising instructions to:
3 assign a severity level to the port scan and report the severity level of the
4 port scan.

1 22. (Original) The computer program product of claim 21 wherein the
2 reported severity varies as a function of the deviation from historical norm.

1 23. (Currently amended) The computer program product of claim 21
2 further comprising instructions to:
3 determine from the ~~connection table~~ first data structure statistics about
4 TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in
5 the number of RST packets and ICMP port-unreachable packets ~~relative to the~~
6 profile to increase determine the severity of a port scan event.

1 24. (Currently amended) Apparatus comprising:
2 circuitry for detecting scanning attacks, comprising:
3 circuitry to add host-pair connection records to a ~~connection table~~first data
4 structure when a host accesses another host during a first update period;
5 ~~circuitry to access the connection table to determine new host pairs;~~
6 circuitry to determine the number of new host pairs added to the
7 ~~connection table~~first data structure over a first update period; and
8 circuitry to aggregate host-pair connection records from the first data
9 structure into a second data structure which corresponds to a second update period
10 that is greater than the first update period;
11 circuitry to determine the number of new host pairs added to the second
12 data structure over the second update period; and
13 circuitry to indicate a host as a scanner when at least one of the following
14 conditions is true:
15 (1) the host appears in more than a first threshold number of host pairs
16 within the first update period, and a first historical number of host pairs is smaller
17 than the first threshold number by a first factor value; and
18 (2) the host appears in more than a second threshold number of host pairs
19 within the second update period, and a second historical number of host pairs is
20 smaller than the second threshold number by a second factor value.~~circuitry to~~
21 ~~indicate to a console that the new host is a scanner when a host has made more~~
22 ~~than a first threshold number “C1” host pairs, and an historical number of host~~
23 ~~pairs is smaller than the threshold number by a first factor value “C2.”~~

1 25. (Currently amended) The apparatus of claim 24 wherein “C1” and
2 ~~“C2”~~the first threshold number and the first factor value are adjustable thresholds.

1 26. (Currently amended) The apparatus of claim 24 wherein the
2 ~~connection table~~first data structure is a current time-slice connection table and
3 ~~host-pair~~host-pair connection records are added to the current time slice
4 connection table.

1 27. (Currently amended) The apparatus of claim 24, further comprising:
2 ~~circuitry to aggregate records from the current time slice table into a~~
3 ~~second update period table;~~
4 circuitry to check for ping scans at the end of a second update period; and
5 circuitry to indicate hosts which produced more than “C3”the second
6 threshold number of new host pairs over the second update period.

1 28. (Currently amended) Apparatus comprising:
2 a processing device; and
3 a computer readable medium tangible embodying a computer program
4 product for detecting scanning attacks, the computer program product comprising
5 instructions for causing the processing device to:
6 add host-pair connection records to a ~~connection table~~first data structure
7 when a host accesses another host during a first update period;
8 ~~at the end of a first update period, accessing the connection table to~~
9 ~~determine new host pairs;~~
10 determine the number of new host pairs added to the ~~connection table~~first
11 data structure over the first update period;~~and~~
12 aggregate host-pair connection records from the first data structure into a
13 second data structure which corresponds to a second update period that is greater
14 than the first update period;
15 determine the number of new host pairs added to the second data structure
16 over the second update period; and

17 indicate a host as a scanner when at least one of the following conditions
18 is true:
19 (1) the host appears in more than a first threshold number of host pairs
20 within the first update period, and a first historical number of host pairs is smaller
21 than the first threshold number by a first factor value; and
22 (2) the host appears in more than a second threshold number of host pairs
23 within the second update period, and a second historical number of host pairs is
24 smaller than the second threshold number by a second factor value, if a host has
25 made more than a first threshold number “C1” host pairs, and an historical
26 number of host pairs is smaller than the threshold number by a first factor value
27 “C2”, then
28 indicate to a console that the new host is a scanner.

1 29. (Currently amended) The apparatus of claim 28 wherein “C1” and
2 “C2” the first threshold number and the first factor value are adjustable thresholds.

1 30. (Currently amended) The apparatus of claim 28 wherein the
2 connection table first data structure is a current time-slice connection table and
3 host pair host-pair connection records are added to the current time slice
4 connection table.

1 31. (Previously Presented) The apparatus of claim 28, wherein the
2 computer program product further comprises instructions to:
3 aggregate records from the current time slice table into a second update
4 period table;
5 check for ping scans at the end of a second update period; and
6 indicate hosts which produced more than second threshold number of “C3”
7 new host pairs over the second update period.

1 32. (Cancelled)

1 33. (Currently amended) Apparatus comprising:

2 a processing device;

3 a computer readable medium tangibly embodying a computer program

4 product for detecting port scanning attacks, the computer program product

5 comprises instructions for causing a processor to:

6 retrieve from a ~~connection table~~first data structure logged values of
7 protocols and ports used ~~for host-pair connections in host-pair connection records~~
8 in the first data structure during a first update period in the connection table;

9 determine the number of ports associated with a host over the first update
10 period based on the host-pair connection records in the first data structure;

11 aggregate host-pair connection records from the first data structure into a
12 second data structure which corresponds to a second update period that is greater
13 than the first update period;

14 determine the number of ports associated with a host over the second
15 update period based on the host-pair connection records in the second data
16 structure; and

17 report a host associated with a port scan when at least one of the following
18 conditions is true:

19 (1) the number of ports associated with the host within the first update
20 period is greater than a first threshold number, and a first historical number of
21 ports associated with the host is smaller than the first threshold number by a first
22 factor value; and

23 (2) the number of ports associated with the host within the second update
24 period is greater than a second threshold number, and a second historical number
25 of ports associated with the host is smaller than the second threshold number by a
26 second factor value;~~determine if the number of ports used in a historical profile is~~
27 ~~smaller by a factor "C1" than a current number of ports being scanned by a host~~

28 ~~and the current number is greater than a lower bound threshold “C2”, to record~~
29 ~~the anomaly; and~~
30 ~~report a port scan to a console.~~

1 34. (Original) The apparatus of claim 33 further comprising instructions
2 to:
3 assign a severity level to the port scan and report the severity level of the
4 port scan.

1 35. (Currently amended) The apparatus of claim 34 wherein the reported
2 severity varies as a function of the deviation from a historical norm ~~as determined~~
3 ~~from the historical profile.~~

1 36. (Currently amended) The apparatus of claim 34 further comprising
2 instructions to:
3 determine from the ~~connection table~~first data structure statistics about
4 TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in
5 the number of RST packets and ICMP port-unreachable packets ~~relative to the~~
6 ~~profile to increase~~determine the severity of a port scan event.

1 37. (New) A computer implemented method of detecting scanning attacks,
2 comprises:
3 adding host-pair connection records to a first data structure stored on a
4 computer readable medium when a host accesses another host during a first
5 update period;
6 determining the number of new host pairs added to the first data structure
7 over the first update period;
8 aggregating host-pair connection records from the first data structure into

9 a second data structure which corresponds to a second update period that is
10 greater than the first update period;
11 determining the number of new host pairs added to the second data
12 structure over the second update period; and
13 indicating a host as a scanner when the host appears in more than a first
14 threshold number of host pairs within the first update period, and a first historical
15 number of host pairs is smaller than the first threshold number by a first factor
16 value.

1 38. (New) A computer implemented method of detecting scanning attacks,
2 comprises:
3 adding host-pair connection records to a first data structure stored on a
4 computer readable medium when a host accesses another host during a first
5 update period;
6 determining the number of new host pairs added to the first data structure
7 over the first update period;
8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period;
11 determining the number of new host pairs added to the second data
12 structure over the second update period; and
13 indicating a host as a scanner when the host appears in more than a second
14 threshold number of host pairs within the second update period, and a second
15 historical number of host pairs is smaller than the second threshold number by a
16 second factor value.

1 39. (New) A computer implemented method of detecting port scanning
2 attacks, the method comprises:

3 retrieving from a first data structure stored on a computer readable
4 medium logged values of protocols and ports in host-pair connection records
5 added in the first data structure during a first update period;
6 determining the number of ports associated with a host over the first
7 update period based on the host-pair connection records in the first data structure;
8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period;
11 determining the number of ports associated with a host over the second
12 update period based on the host-pair connection records in the second data
13 structure; and
14 reporting a host associated with a port scan when the number of ports
15 associated with the host within the first update period is greater than a first
16 threshold number, and a first historical number of ports associated with the host is
17 smaller than the first threshold number by a first factor value.

1 40. (New) A computer implemented method of detecting port scanning
2 attacks, the method comprises:
3 retrieving from a first data structure stored on a computer readable
4 medium logged values of protocols and ports in host-pair connection records
5 added in the first data structure during a first update period;
6 determining the number of ports associated with a host over the first
7 update period based on the host-pair connection records in the first data structure;
8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period;
11 determining the number of ports associated with a host over the second
12 update period based on the host-pair connection records in the second data
13 structure; and

14 reporting a host associated with a port scan when the number of ports
15 associated with the host within the second update period is greater than a second
16 threshold number, and a second historical number of ports associated with the
17 host is smaller than the second threshold number by a second factor value.